

IKT-reglement for UMB

12. mai 2005

*Basert på:
«IKT-reglement for institusjoner i utdanningssektoren»
UNINETT FAS/UNINETT ABC
Versjon 1.0, 1. desember 2004*

Innhold

Overordnet reglement for bruk av IKT	3
Subreglement	
1. Eierskap og behandling av data	5
2. Utlevering av opplysninger	7
3. Ressursbruk	8
4. Brukerens plikt til å identifisere seg	10
5. Sanksjoner	11
8. Inngrep	12
7. Brukerregistrering	14
8. Saksbehandling	16
Vedlegg	
Definerte brukerroller ved UMB	

Overordnet reglement for bruk av IKT

Nedslagsfelt:

Dette reglementet gjelder for bruk av UMBs IKT-ressurser. Reglementet gjelder også bruk av andres IKT-ressurser gjennom bruk av sin tilknytning til UMBs.

Bruk av IKT-ressurser:

Bruk av UMBs IKT-ressurser er ment å skulle oppfylle UMBs formål. Det er forbudt å bruke UMBs IKT-ressurser til noe som er uforenlig med UMBs formål, eller med de etiske eller moralske normene som er fastsatt for UMB. Bruk av UMBs IKT-ressurser til noe som strider mot norsk lov vil kunne føre til selvstendige sanksjoner fra UMB.

Det er ikke tillatt å bruke UMBs IKT-ressurser uten å få tillatelse til dette i forkant. Det å få en bruker hos UMB innebærer at tillatelse er gitt til formålstjenlig bruk.

Det er ikke tillatt å bruke UMBs IKT-ressurser på en måte som opptar større ressurser enn nødvendig, tatt de tilgjengelige ressursene i betraktning. Bruk som ikke er begrunnet i UMBs formål skal ikke oppta annet enn ubetydelige ressurser.

IKT-ressursene skal ikke brukes på en måte som kan forringe eller krenke deres integritet. Dette gjelder også ved bruk av privat utstyr.

Brukere har plikt til å følge IKT-ansattes pålegg og instruksjoner om bruk av IKT-ressursene. Hvor det er påkrevd skal brukere identifisere seg på korrekt måte. En brukers passord eller annen nøkkel skal holdes hemmelig og skal kun anvendes av den korrekte brukeren.

Vis nett-vett.

Brukernes rettigheter

UMB skal sette klare standarder og retningslinjer for hva som er forsvarlig bruk av UMBs IKT-ressurser.

UMB skal tilgjengeliggjøre oppdatert informasjon til brukerne om relevante forhold om IKT-ressursene og brukernes anvendelse av disse.

Alle brukere har krav på at deres personvern og integriteten til deres data ikke krenkes av UMB. UMB skal bidra til at brukernes personvern og integriteten til brukernes data ikke krenkes av andre.

UMB skal ikke utlevere opplysninger om en enkelt bruker eller data tilhørende en bruker hvor dette ikke fremgår av vedtatte reglementer eller følger av lovgivningen forøvrig.

Inngrep og sanksjoner

Brudd på IKT-reglementet kan føre til sanksjoner fra UMB. Straff eller sanksjoner grunnet bruk av IKT-ressurser skal ikke avvike fra sanksjoner grunnet annen opptreden ved UMB. Sanksjoner skal fastsettes av ansvarlig enhet.

IKT-driftspersonell har som oppgave å sikre systemets funksjonalitet og integritet. IKT-driftspersonell ved UMB kan utføre ethvert inngrep for å ivareta systemets funksjonalitet så lenge som det ikke er i utrensmål. Ved inngrep skal bruker varsles så snart som praktisk mulig.

Ansvarsfraskrivelse:

UMB er ikke ansvarlig for noe tap av data, tjenestebortfall eller andre tap som skyldes svikt i IKT-tjenestene. UMB kan ikke frata brukere rettigheter eller stille dem til ansvar grunnet handlinger eller passivitet hvor det er svikt i IKT-tjenestene som er årsaken til dette.

Del IV Subreglementer

1. Eierskap og behandling av data
2. Utlevering av opplysninger
3. Ressursbruk
4. Brukerens plikt til å identifisere seg
5. Sanksjoner
6. Inngrep
7. Brukerregistrering
8. Saksbehandling

<i>Reglement</i>	<i>Dato</i>	<i>Gitt av</i>	<i>Hjemmel</i>
Eierskap og utlevering av data	12.05.2005	Universitetsstyret	US-sak 83/2005

Dette reglementet dekker ikke logger ol. som er UMBs eiendom.

Utgangspunkt:

UMB forholder seg til en fil sin eier som en indikasjon på hvem som eier data. Om eierskapet er korrekt eller ikke, skal ikke dette på noe vis endre det reelle eierskapet til data.

Eierskap til data

UMB forholder seg til at den som er oppført som eier av en fil, er disse datas eier. Dette uansett hvor filen skulle befinne seg. UMB vil kun utlevere filen til den som er oppført som eier med mindre det ved beslutning av norsk domstol bestemmes noe annet.

Konflikt om eierskap til data mellom to 3. parter

Hvor to parter begge hevder å være eier til data vil UMB i utgangspunktet utlevere data til parten som er oppført som eier av filen. Hvor en part varsler rettslige skritt for å få fastslått eierskapet kan UMB allikevel i en kortere periode avvente utleveringen.

Hvis ikke en avgjørelse fattes, får ingen utlevert noe?

Hvor det ikke er mulig å sannsynliggjøre hvem som eier data, og flere hevder å ha eiendomsretten til nevnte data, vil det ikke bli utlevert noe før det foreligger en avgjørelse fra norsk domstol omkring eierskapet til dataene.

Utlevering av data ved brukerforholdets opphør

Brukerforholdets opphør grunnet brukerens tilknytning til UMB

Hvor brukerens forhold til UMB opphører, f.eks. ved endt studium eller avsluttet arbeidsforhold skal brukeren selv besørge å fjerne sine data fra UMB IKT-ressurser, herunder å ta kopier av de data brukeren ønsker å beholde. Brukeren skal derfor ha tilgang til sine data i tre måneder etter at rollen som begrunnet brukerforholdet opphørte. I løpet av denne perioden må brukeren motta varsel om at kontoen vil bli slettet og at alle data vil forsvinne. Etter dette skal UMB vente i ytterligere tre måneder før kontoen inklusive all data blir slettet.

At brukeren skal ha tilgang til sine data betyr ikke at andre tjenester skal være tilgjengelige.

Brukerforholdets opphør grunnet brukerens død

Hvor en bruker dør, vil dennes arvinger (dødsboet) tre inn i dennes sted hva angår rettigheter knyttet til såvel fysiske som immaterielle goder og objekter. Retten til innholdet av dennes hjemmeområde er et slikt.

Det som må fastlegges er at den eller de som ønsker å få utlevert innholdet av hjemmeområdet er rett arving. Dette gjøres ved fremleggelse av en skifteattest, hvor det fremgår hvem arvingene er.

Personlig innhold skal lagres på hjemmeområde. Materiale som lagres på arbeidsplassmaskin vil uten gjennomgåelse av hva det inneholder, bli slettet ved en brukers død.

Prosedyre for utlevering av data

Utfylling av erklæring

Utlevering skjer mot utfylling av en erklæring hvor mottaker av data underskriver på at denne

- Har mottatt data
- Erkjenner at overleveringen ikke medfører noen endring i faktiske eierforhold.
- Lover å utlevere data som tilhører andre til riktig mottaker

Arkivering

En kort redegjørelse (f.eks en logg) for utleveringen, samt kopi av dokumenter som identifiserer rett mottaker (f.eks. skifteattest), erklæring og andre relevante dokumenter skal arkiveres.

Utlevering

Utlevering skjer på egnet medium som kan deles ut i bytte mot erklæring.

<i>Reglement</i>	<i>Dato</i>	<i>Gitt av</i>	<i>Hjemmel</i>
Utlevering av logger eller liknede informasjon	12.05.2005	Universitetsstyret	US-sak 83/2005

Utlevering av opplysninger

Det vil med jevne mellomrom kunne komme klager eller henvendelser rettet til UMB hvis mål er å få utlevert logger eller informasjon (identitet) om en bruker. Dette er i utgangspunktet ikke noe man skal gi ut. Mange av opplysningene er belagt med taushetsplikt, men også andre regler, f.eks. etter personopplysningsloven tilsier at stor forsiktighet skal utvises i forhold til utlevering av informasjon om enkeltpersoner eller om deres bruk av IKT-ressurser.

Spesielt om utlevering til politi eller påtalemyndighet

Etter Ekomlovens §2-9 kan politi eller påtalemyndighet kreve å få identifisert en bruker av et ip-nummer. Andre data, f.eks. logger av trafikkdata eller innholdet i kommunikasjoner krever beslutning av en domstol.

Utlevering til andre

Utlevering opplysninger, logger eller likende til andre enn politi eller påtalemyndigheter krever beslutning fra norsk domstol.

Utlevering til brukeren selv

En bruker som ønsker utlevert seg opplysninger, logger eller likende som omhandler denne selv, kan få dette ved vanlig henvendelse til IKT-seksjonen. Retten til dette følger bla. av personopplysningsloven.

Fellestjenester i sektoren

For fellestjenester i sektoren, herunder en brukers utnyttelse av andre institusjoners IKT-ressurser vil eventuelt misbruk enten bli tatt hånd om av brukerens vertsinstitusjon ved klage på denne fra UMB hvis ressurser er misbrukt, eller UMB hvis ressurser er misbrukt kan forfølge saken i rettsvesenet og dermed få identifisert brukeren etter reglene over.

<i>Reglement</i>	<i>Dato</i>	<i>Gitt av</i>	<i>Hjemmel</i>
Utnyttelse av IKT-ressurser	12.05.2005	Universitetsstyret	US-sak 83/2005

Utgangspunkt.

Bruk av UMBs IKT-ressurser skal hovedsakelig forekomme for å fremme UMBs formål.

Det er ikke tillatt å bruke UMBs IKT-ressurser på en måte som opptar større ressurser enn nødvendig, tatt de tilgjengelige ressursene i betraktning. Bruk som ikke er begrunnet i UMBs formål skal ikke oppta annet enn ubetydelige ressurser.

Tillatt bruk etter UMBs formål.

Formålet til UMBs er utdanning, forskning og formidling.

Bruk som er direkte relatert til UMBs formål er grunnlaget for de ressursene som er tilgjengelige og er derfor tillatt så lenge som det ikke opptar for store ressurser slik at bruken blir til fortrensel for annen tillatt bruk.

Bruk som ikke er direkte relatert til UMBs formål er kun tillatt i den utstrekning det opptar ubetydelige ressurser. Bruk som ikke har noen beskyttelsesverdige interesse kan forbys av IKT-seksjonen.

Privat bruk

IKT-tjenestene ved UMB er hovedsakelig til bruk for å oppfylle formålet til UMB. Imidlertid er det fullt ut akseptabelt at brukere anvender IKT-ressursene til private gjøremål så lenge som de ikke

- opptar IKT-ressurser på bekostning av annet bruk.
- bryter lisenser, avtalevilkår eller andre forutsetninger
- bidrar til å svekke sikkerhet eller stabilitet
- er forbudt av IKT-seksjonen

Kommersiell bruk

Bruk av UMBs IKT-ressurser til kommersielle formål (enhver form for kjøp, salg, utleie, annonsering mot betaling eller likende) er forbudt med mindre det foreligger skriftlig tillatelse til slik bruk i forkant.

Ingen beskyttelsesverdig interesse

Handlinger som anvender IKT-ressurser men ikke er begrunnet utifra beskyttelsesverdige interesser slik som UMBs formål eller alment aksepterte interesser kan forbys av IKT-seksjonen. Hvor det er grunn til å klandre brukeren for handlingen, kan sanksjoner iverksettes. Avveiningen skal foretas etter momentene gjengitt under:

En handling har ikke beskyttelsesverdige interesser i denne konteksten hvor den ikke har en særlig nærhet til UMBs formål og heller ikke har en særlig nærhet til alminnelig anerkjente rettigheter eller formål slik som:

- demokrati
- grunnleggende rettigheter
- samfunnsøkonomisk nytte
- tekniske eller andre vitenskapelige fremskritt

Handlingen vil kunne være i strid med dette reglementet hvor den samtidig anvender UMBs IKT-ressurser.

IKT-seksjonen kan iverksette sanksjoner mot en bruker som har foretatt en slik handling hvor:

- En vanlig oppegående bruker forsto eller burde ha forstått at handlingen ikke var tillatt bruk av IKT-ressursene

og

- Handlingen ikke utelukkende eksisterte i brukerens privatsfære.

Håndheving av ressursutnyttelse.

Enhver enhet og hver enkelt bruker har et selvstendig ansvar for å selv påse at egen bruk er innenfor grensene av tillatt bruk. IKT-seksjonen kan og skal gi generelle retningslinjer om hvilket bruk som tillates.

I spesielle tilfeller hvor IKT-seksjonen blir oppmerksom på bruk som, etter en konkret vurdering basert på nærheten til UMBs formål, andre beskyttelsesverdige interesser og mengden ressurser bruken opptar, ikke bør tillates, skal IKT-seksjonen sørge for at denne stoppes. Hvis det er grunn til å klandre en bruker for opptreden i forbindelse med slik bruk kan sanksjoner fra IKT-seksjonen iverksettes mot brukeren.

<i>Reglement</i>	<i>Dato</i>	<i>Gitt av</i>	<i>Hjemmel</i>
Brukerens plikt til å identifisere seg	12.05.2005	Universitetsstyret	US-sak 83/2005

Korrekt identifikasjon

Alle brukere plikter å til enhver tid identifisere seg selv på en korrekt måte ovenfor UMB hvor det er lagt opp til dette. Det er forbudt å identifisere seg eller å forsøke å identifisere seg som en annen enn den man er.

Riktig brukernavn

For alle tjenester hos UMB hvor en skal identifisere seg selv skal kun ens eget brukernavn anvendes.

Riktig avsenderadresse

Det er forbudt å forsøke å modifisere eller skjule noen felt eller informasjon i noen kommunikasjon med sikte å å skjule hvor den kommer fra, eller gi et feilaktig bilde av dette.

Riktig maskinnavn/ip- adresse

Det er forbudt å forsøke å endre en innstilling, aksessere tjenester via omveier eller på andre måter forsøke å skjule hvilken maskin en sitter ved eller gi et feilaktig inntrykk av dette ovenfor UMB eller andre brukere tilknyttet UMB.

Hemmeligholdelse av nøkkel

Det er svært viktig å holde sin nøkkel hemmelig. Denne eksisterer ofte i form av et passord eller en pin-kode. Det er forbudt å dele denne med noen. Hvor det går frem at en nøkkel er blitt kjent vil brukerkonto bli sperret og brukeren vil bli ansvarliggjort.

Retten til anonymitet

Det er ikke opp til UMB å bestemme hvorvidt brukerne identifiserer seg ovenfor tredjemann ved bruk av åpne tjenester utenfor UMB. Dog vil brudd på norsk eller internasjonal lovgivning utført via eller ved hjelp av UMBs IKT-ressurser rammes av IKT-reglementet.

<i>Reglement</i>	<i>Dato</i>	<i>Gitt av</i>	<i>Hjemmel</i>
Sanksjoner mot brukere	12.05.2005	Universitetsstyret	US-sak 83/2005

Sanksjoner

En sanksjoner en reaksjon iverksatt for å straffe en bruker for klanderverdig adferd fra dennes side. Handlingen iverksatt for å oppnå andre resultater, f.eks. stabilitet og sikkerhet blant IKT-ressursene er ikke en sanksjon.

Sanksjoner i forhold til opptreden relatert til IKT-ressurser, skal håndteres av IKT-organisasjonen. Sanksjoner relatert til annen opptreden skal håndteres av brukerens ansvarlige enhet.

Omfang av sanksjoner og kompetanse til å iverksette disse

Styret

En total sperring av en brukerkonto er en bortvisning etter universitetslovens §11.

Styret er tillagt kompetansen til å bortvise en bruker. Saksbehandlingen og prosedyren for å gjøre dette er bestemt av lovverket. Disse må følges i slike tilfeller.

Retten til å ha en operativ brukerkonto som gir tilgang til administrative tjenester, utdanning og tilhørende innleveringer eksamener mv. kan ikke som en sanksjon fratras brukere uten at dette er å anse som en bortvisning. Det samme gjelder retten til å kunne motta kommunikasjoner fra UMB eller noen av dets organer.

Ansvarlig enhet

Den ansvarlige enheten skal ikke iverksette sanksjoner vha. endring av privilegier for bruk av IKT.

IKT-organisasjonen

IKT-seksjonen kan iverksette sanksjoner ved å frata brukere visse begrensede privilegier i en begrenset tidsperiode.

Sanksjoner skal være et resultat av et misbruk og relatert til den misbrukte ressursen.

Førstelinde av IKT-organisasjonen skal ikke iverksette sanksjoner mot brukere utover tilsnakk eller rapportering av dem til 2. linje.

Ved alvorlig misbruk skal IKT-seksjonen eskalere en sak i linjen, via den ansvarlige enheten til styret, for beslutning om bortvisning skal finne sted.

<i>Reglement</i>	<i>Dato</i>	<i>Gitt av</i>	<i>Hjemmel</i>
Inngrep	12.05.2005	Universitetsstyret	US-sak 83/2005

Inngrep

Et inngrep er en faktisk handling som er foretatt for å oppnå noe annet enn å straffe en bruker.

IKT-seksjonen kan foreta inngrep når dette er nødvendig. Med nødvendig menes for å opprettholde sikkerhet, integritet, konfidensialitet og tilgjengeligheten i IKT-systemer, tap av liv helse eller gods, hindre at UMB kommer i ansvar, eller opprettholdelse av UMBs rykte samt det å forhindre rettsbrudd.

Innsyn

Med innsyn menes et fysisk individ som gjennom en manuell prosess skaffer seg tilgang til data som tilhører andre brukere. Automatiske prosesser som foretar handlinger mot store grupper brukere bedriver ikke innsyn. Dette gjelder f.eks. virusscanning eller prosesser som generer rapporter som ikke identifiserer individer.

Filer, områder og logger

Brukerens private sfære strekker seg kun til kunnskap om eksistens av og innhold i filer. Hvilke prosesser en maskin har gående, er informasjon som til enhver til skal være tilgjengelig for driftspersonale.

Logger som inneholder informasjon om prosesser, innlogginger, avvik eller andre hendelser er UMBs eiendom og skal være tilgjengelig for driftspersonale.

Det er et konkret skille mellom brukerens filer og områder, og den logging av diverse ting som en institusjon foretar. Det er ikke et innsyn i så måte å gå gjennom disse, men det må til gjengjeld være slik at UMB ikke logger annet enn det som er forsvarlig, og at dette opplyses om.

Innsyn i data, filer eller områder tilhørende privat bruker

Det er i utgangspunktet kun brukeren selv som har tilgang til dennes data, filer eller private områder.

Samtykke

Som standard er samtykke det man skal be om hvis inngrep med innsyn er nødvendig. I visse tilfeller kan det være nødvendig å skaffe seg dette uten samtykke.

Tillatelse fra overordnet

I en situasjon hvor tidsnød eller andre årsaker umuliggjør eller gjør det svært vanskelig eller u hensiktsmessig å innhente samtykke, kan innsyn foretas med tillatelse av IKT-lederen eller den som opptrer i dennes sted.

Situasjoner med særlig tidsnød

I en situasjon hvor særlig tidsnød eller andre årsaker umuliggjør eller gjør det svært vanskelig eller u hensiktsmessig å innhente tillatelse av IKT-lederen eller den som opptrer i dennes sted, kan innsyn foretas av IKT-personalet.

Informasjon i ettertid

Hvor noen har skaffet seg innsyn i en brukers personlige område uten forutgående samtykke fra brukeren selv skal brukeren straks varsles.

Varslet skal redegjøre for hvilket inngrep som har blitt foretatt, hvilken hjemmel dette hviler på og de særlige forhold som er påberopt.

Registrering av innsyn

At innsyn har vært foretatt skal registreres i saksbehandlingssystem.

Sperring/stengning av ressurser

Hvor et det er nødvendig kan inngrep iverksettes ved å sperre, stenge eller på andre måter endre en ressurs.

Informasjon til brukere

Hvor en ressurs sperres skal brukeren ha beskjed. Dette skal skje så snart som mulig. Hvor ressurser som påvirker mange brukere er sperret, kan innholdet i varsel være identisk. Hvis det er praktisk mulig bør, informasjonen nå alle brukere individuelt. Beskjed skal gis gjennom et kommunikasjonsmiddel som ikke er sperret.

<i>Reglement</i>	<i>Dato</i>	<i>Gitt av</i>	<i>Hjemmel</i>
Reglement for Brukerregistrering	12.05.2005	Universitetsstyret	US-sak 83/2005

Vilkår for å bli bruker

For å bli bruker ved UMB må man ha et formalisert forhold til UMB. Et formalisert forhold har den som er ansatt, opptatt til studier eller har en skriftlig avtale med UMB om sin tilstedeværelse.

For å bli bruker skal et minimumssett av ens persondata finnes i et av de administrative systemene til UMB. Dette kan være studentsystemet eller personalsystemet. De opplysningene som må registreres er:

- navn
- personnummer
- tilknytning / rolle i forhold til UMB
- varighet av tilknytning
- plassering i UMB

Visse typer ansatte kan ha en tilknytning som ikke etter sitt formål behøver å bli bruker av IKT-tjenestene. Dette skal i så fall være grunnet objektive kriterier og utvelgelse skal skje på grunnlag av formelle roller. Dette skal fremgå av registreringen i student- eller personalsystemet.

Registrering av brukere

Ved registrering av nye individer i enten student- eller personalsystem skal det automatisk bygges en bruker til vedkommende. Dette gjelder ikke hvis:

- *det av vedkommendes registrering fremgår at denne ikke skal ha bruker*
- *det allerede finnes en bruker for et individ med den identifikatoren*

Finnes det allerede en bruker og denne skal benyttes, må det sikres at de over nevnte pliktige personopplysninger er tilstede i oppdatert form.

Etter at bruker er bygget skal brukernavn og passord (eller annen autentiseringsinformasjon, f.eks. pin-kode) sendes bruker på sitt arbeids/studiested. Samtidig skal bruker få informasjon om IKT-ressursene og reglene for bruk av disse.

IKT-seksjonen skal som regel ikke bygge brukere som ikke finnes i enten student- eller personalsystem. Unntak fra dette kan skje hvor tekniske forhold nødvendiggjør det. Ved manuell registrering skal også de over nevnte pliktige personopplysninger registreres. Manuelt opprettede brukere skal ikke være gyldige i mer enn ett år.

Det kan settes som vilkår at bruker ved første anvendelse / aktivering av brukerkonti selv velger et nytt passord/pinkode el. l.

Varighet av brukerforhold

En brukers konto ved UMB skal ha en like lang varighet som tilknytningen brukeren har til UMB har. I tillegg kan brukeren få tre måneder til å rydde opp i sine forhold før kontoen blir sperret.

Opphør av brukerforhold

Ved opphør av brukers tilknytning etter registrering enten student eller personalsystem skal brukeren varsles om at kontoen sperres om 3 måneder og at brukeren i denne perioden må ta

sikkerhetskopi av alle filer brukeren ønsker å beholde¹.

Etter 3 måneder sperres brukers konto. Etter ytterligere seks måneder slettes brukers konto. Sikkerhetskopierte data slettes etter 5 år.

¹ Se «eierskap til data»

<i>Reglement</i>	<i>Dato</i>	<i>Gitt av</i>	<i>Hjemmel</i>
Saksbehandling	12.05.2005	Universitetsstyret	US-sak 83/2005

Alminnelige regler ved saksbehandling

IKT-ansatte er underlagt de alminnelige saksbehandlingsreglene som gjelder i det offentlige hva angår utøvelse av myndighet som ansatt av forvaltningsorgan.

Taushetsplikt

IKT-ansatte er underlagt taushetsplikt etter forvaltningslovens § 13. Taushetsplikten gjelder for alle taushetsbelagte opplysninger som en får kjennskap til gjennom utøvelse av sin stilling. Taushetsplikten gjelder også mot andre ansatte i IKT-organisasjonen, unntatt oppover i linjen.

Arkiveringsplikt

Dokumenter tilhørende sak hvis behandling utgjør et enkeltvedtak etter forvaltningsloven §2b er arkivverdig og skal arkiveres i offentlig journal. Ved tvil om hvorvidt en sak er arkivverdig eller ei skal arkivpersonale rådføres.

Innsynsrett

Alle har rett til innsyn i offentlig journal jmf. offentlighetsloven § 2.

Alle som er part i en sak har innsyn i sakens dokumenter. Innsynet gjelder ikke dokumenter og kommunikasjon for intern saksforberedelse.

Svarplikt mm.

UMB plikter å besvare alle henvendelser rettet til det som forvaltningsorgan eller institusjon. Dette gjelder ikke masseutsendte kommunikasjoner i markedsføringsøyemed (SPAM).

Alle henvendelser skal besvares innen rimelig tid.

UMB plikter å gi alminnelig veiledning til brukerne som er relevant i forhold til mottatte henvendelser. Slik veiledning kan være henvisning til tilgjengelig informasjon. I saker hvor det utøves forvaltningsmyndighet skal det fremgå at brukerne har adgang til å klage på enkeltvedtak.

Gjentatte henvendelser i saker som er avgjort og hvor det ikke er videre klageadgang, er ikke tillatt. Ei heller gjentatte meningsyttringer til slike kanaler, hvor svar på slike allerede har blitt gitt. Det er ikke pliktig å besvare slike henvendelser annet enn med en standardisert avvisning.

Elektronisk kommunikasjon

Det skal fremgå tydelig, for eksempel på UMBs hjemmeside, hvilke kanaler og adresser som kan benyttes til å rette henvendelser til UMB ved hjelp av elektronisk kommunikasjon. UMBs angitte inngående kommunikasjonskanaler skal leses av mennesker og ikke være gjenstand for maskinell fjerning av kommunikasjoner.

Vedlegg til IKT-reglement for UMB

Retningslinjer

12. mai 2005

Definerte brukerroller ved UMB

Utgangspunkt:

Dette vedlegget til IKT-reglementet definerer hvilke brukerroller UMB til en hver tid har i henhold til IKT-reglementets subreglement nr. 7: Brukerregistrering.

Vedlegget kan endres administrativt.

Definerte brukerroller:

Ansatt

Beskrivelse:	Bruker som har ansettelsesforhold ved UMB
Legitimerende enhet:	PoA, Lønns- og personalsystemet
Rettighetsnivå:	Basis - Fagnett (vLan10). Gruppemedlemskap for ytterligere rettigheter
Varighet:	ikke begrenset. Opphører når ansettelsesforholdet opphører (iht Paga)
Opphørsprosedyre:	Kontoer stenges ved opphør. Personlige data (iht subreglement 2) skal ivaretas av brukeren innen opphør. Etter stengning er kontoene tilgjengelige (etter avtale) i 3 mnd. Utover dette arkiveres dataene inntil 1 år etter opphørsdato.
Kommentar:	Benyttes ikke ved kortvarige kontrakter inntil 1mnd. Stipendiater ansatt ved UMB regnes som ansatte.

Student

Beskrivelse:	Bruker som har studenttilknytning til UMB, inklusive stipendiater.
Legitimerende enhet:	Studieavdelingen, FS (Felles Studentsystem)
Rettighetsnivå:	Studentnett (vLan30).
Varighet:	Ikke begrenset. Opphører når studenttilknytningen opphører (iht FS).
Opphørsprosedyre:	Kontoer stenges ved opphør. Personlige data (iht subreglement 2) skal ivaretas av brukeren innen opphør. Etter stengning er kontoene tilgjengelige (etter avtale) i 3 mnd. Utover dette arkiveres dataene inntil 1 år etter opphørsdato.
Kommentar:	Stipendiater som har behov for utvidede rettigheter må i tillegg defineres i «assosiert»-rollen.

Assosiert

Beskrivelse:	Bruker med avtalefestet tilknytning til en enhet på UMB, hvor det er behov for arbeidsplass ved UMB.
Legitimerende enhet:	Enhet som har inngått avtale.
Rettighetsnivå:	Etter avtale.
Varighet:	Tidsbegrenset. Varighet kan settes inntil 2 år. Ved eventuell utvidelse skal ny tidsbegrensning settes.
Opphørsprosedyre:	Kontoer stenges ved opphør. Personlige data (iht subreglement 2) skal ivaretas av brukeren innen opphør. Etter stengning er kontoene tilgjengelige (etter avtale) i 3 mnd. Utover dette arkiveres dataene inntil 1 år etter opphørsdato.
Kommentar:	Rollen «assosiert» er mer forpliktende enn «gjest». Det kreves derfor at

legitimerende enhet har skriftlig avtale som beskriver vedkommendes funksjon og behov ved UMB.

Gjest

Beskrivelse: Bruker med kortvarig opphold ved UMB.
Legitimerende enhet: Enhet som har invitert eller på annen måte har avtale med vedkommende.
Rettighetsnivå: Kun gjestenett (vLan 95).
Varighet: Tidsbegrenset.
Opphørsprosedyre: Det opprettes ingen kontoer, og det er dermed ikke data som skal fjernes.
Kommentar:

Kursbruker

Beskrivelse: Deltaker på etter- og videreutdanningskurs (uten FS-tilknytning).
Legitimerende enhet: SEVU / kursførende enhet.
Rettighetsnivå: pålogging på datasal.
Varighet: Tidsbegrenset til kursets varighet.
Opphørsprosedyre: Kontoer stenges ved opphør. Ingen personlige data blir arkivert.
Kommentar:

Pensjonist

Beskrivelse: Tidligere ansatt ved UMB som har avtale om arbeidsplass ved UMB.
Legitimerende enhet: Aktuell enhet.
Rettighetsnivå: Etter avtale.
Varighet: Tidsbegrenset, maks 2 år. Ved utvidelse skal ny tidsbegrensning settes.
Opphørsprosedyre: Kontoer stenges ved opphør. Personlige data (iht subreglement 2) skal ivaretas av brukeren innen opphør. Etter stengning er kontoene tilgjengelige (etter avtale) i 3 mnd. Utover dette arkiveres dataene inntil 1 år etter opphørsdato.
Kommentar: Rollen faller i prinsippet inn under «assosiert», men er et såvidt vanlig spesialtilfelle at det er hensiktsmessig med egen rolle, hvor det heller ikke stilles samme krav til kontrakt.

IT-adm

Beskrivelse: Bruker ved IT-seksjonen som er knyttet til IT-administrasjon.
Legitimerende enhet: Aktuell enhet.
Rettighetsnivå: Fagnett (vLan10) + administrative rettigheter.
Varighet: Tidsbegrenset, maks 2 år. Ved utvidelse skal ny tidsbegrensning settes.
Opphørsprosedyre: Kontoer stenges ved opphør. Personlige data (iht subreglement 2) skal ivaretas av brukeren innen opphør. Etter stengning er kontoene tilgjengelige (etter avtale) i 3 mnd. Utover dette arkiveres dataene inntil 1 år etter opphørsdato.
Kommentar: Rollen faller i prinsippet inn under «assosiert», men er et såvidt vanlig spesialtilfelle at det er hensiktsmessig med egen rolle, hvor det heller ikke stilles samme krav til kontrakt.

Funksjonsbruker

- Beskrivelse: Brukerkonto knyttet til funksjon og ikke til person. Kontoen er uavhengig av personlige konti og kan benyttes av flere i en gruppe. En funksjonskonto må likevel ha en ansvarlig eier.
- Legitimerende enhet: Aktuell enhet.
- Rettighetsnivå: Avhengig av funksjon.
- Varighet: Ikke tidsbegrenset, men knyttes til ansvarlig eier.
- Opphørsprosedyre: Konto deaktiveres når ansvarlig eier opphører. Det er ingen personlige data knyttet til en funksjonskonto.
- Kommentar: